CLI Commands

The Cisco Wireless LAN solution command-line interface (CLI) enables operators to connect an ASCII console to the Cisco Wireless LAN Controller and configure the controller and its associated access points.

show Commands

show capwap reap association

To display the list of clients associated with an access point and their SSIDs, use the **show capwap reap association** command.

show capwap reap association

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to display clients associated to an access point and their SSIDs:

```
(Cisco Controller) >show capwap reap association
```

show capwap reap status

To display the status of the FlexConnect access point (connected or standalone), use the **show capwap reap status** command.

show capwap reap status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to display the status of the FlexConnect access point:

```
(Cisco Controller) >show capwap reap status
```

show flexconnect acl detailed

To display a detailed summary of FlexConnect access control lists, use the **show flexconnect acl detailed** command.

show flexconnect acl detailed *acl-name*

Syntax Description

acl-name	Name of the access control list.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to display the FlexConnect detailed ACLs:

```
(Cisco Controller) >show flexconnect acl detailed acl-2
```

show flexconnect acl summary

To display a summary of all access control lists on FlexConnect access points, use the **show flexconnect acl summary** command.

show flexconnect acl summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to display the FlexConnect ACL summary:

```
(Cisco Controller) >show flexconnect acl summary
ACL Name                         Status
-------------------------------- -------
acl1                            Modified
acl10                           Modified
acl100                          Modified
acl101                          Modified
acl102                          Modified
acl103                          Modified
acl104                          Modified
acl105                          Modified
acl106                          Modified
```

show flexconnect group detail

To display details of a FlexConnect group, use the **show flexconnect group detail** command.

show flexconnect group detail *group_name*

Syntax Description

group_name	IP address of the FlexConnect group.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to display the detailed information for a specific FlexConnect group:

```
(Cisco Controller) >show flexconnect group detail 192.12.1.2
Number of Ap’s in Group:  1
00:0a:b8:3b:0b:c2   AP1200    Joined
Group Radius Auth Servers:
 Primary Server Index .................... Disabled
 Secondary Server Index .................. Disabled
```

show flexconnect group summary

To display the current list of FlexConnect groups, use the **show flexconnect group summary** command.

show flexconnect group summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to display the current list of FlexConnect groups:

```
(Cisco Controller) >show flexconnect group summary
flexconnect Group Summary:  Count 1
Group Name        # APs
Group 1       1
```

show flexconnect office-extend

To displays information about OfficeExtend access points that in FlexConnect mode, use the **show flexconnect office-extend** command.

show flexconnect office-extend {**summary** | **latency**}

Syntax Description

summary	Displays a list of all OfficeExtend access points.
latency	Displays the link delay for OfficeExtend access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to display information about the list of FlexConnect officeExtend access points:

```
(Cisco Controller) >show flexconnect office-extend summary
Summary of OfficeExtend AP
AP Name            Ethernet MAC       Encryption  Join-Mode   Join-Time
------------------ -----------------  ----------  ----------- ----------
AP1130             00:22:90:e3:37:70   Enabled    Latency     Sun Jan 4 21:46:07 2009
AP1140             01:40:91:b5:31:70   Enabled    Latency     Sat Jan 3 19:30:25 2009
```

The following example shows how to display the FlexConnect officeExtend access point’s link delay:

```
(Cisco Controller) >show flexconnect office-extend latency
Summary of OfficeExtend AP link latency
AP Name              Status  Current   Maximum   Minimum
--------------------------------------------------------------------------
AP1130               Enabled 15 ms      45 ms     12 ms
AP1140               Enabled 14 ms     179 ms     12 ms
```

config Commands

config ap autoconvert

To automatically convert all access points to FlexConnect mode or Monitor mode upon associating with the Cisco WLC, use the **config ap autoconvert** command.

config ap autoconvert {**flexconnect** | **monitor** | **disable**}

Syntax Description

flexconnect	Configures all the access points automatically to FlexConnect mode.
monitor	Configures all the access points automatically to monitor mode.
disable	Disables the autoconvert option on the access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When access points in local mode connect to a Cisco 7500 Series Wireless Controller, they do not serve clients. The access point details are available in the controller. To enable access points to serve clients or perform monitoring related tasks when connected to the Cisco 7500 Series Wireless Controller, the access points must be in FlexConnect mode or Monitor mode.

Examples

The following example shows how to automatically convert all access points to the FlexConnect mode:

```
(Cisco Controller) >config ap autoconvert flexconnect
```

The following example shows how to disable the autoconvert option on the APs:

```
(Cisco Controller) >config ap autoconvert disable
```

config ap flexconnect central-dhcp

To enable central-DHCP on a FlexConnect access point in a WLAN, use the **config ap flexconnect central-dhcp** command.

config ap flexconnect central-dhcp *wlan_id cisco_ap* [**add** | **delete**] {**enable** | **disable**} **override dns** {**enable** | **disable**} **nat-pat** {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
cisco_ap	Name of the Cisco lightweight access point.
add	(Optional) Adds a new WLAN DHCP mapping.
delete	(Optional) Deletes a WLAN DHCP mapping.
enable	Enables central-DHCP on a FlexConnect access point. When you enable this feature, the DHCP packets received from the access point are centrally switched to the controller and then forwarded to the corresponding VLAN based on the AP and the SSID.
disable	Disables central-DHCP on a FlexConnect access point.
override dns	Overrides the DNS server address on the interface assigned by the controller. When you override DNS in centrally switched WLANs, the clients get their DNS server IP address from the AP and not from the controller.
enable	Enables the Override DNS feature on a FlexConnect access point.
disable	Disables the Override DNS feature on a FlexConnect access point.
nat-pat	Network Address Translation (NAT) and Port Address Translation (PAT) that you can enable or disable.
enable	Enables NAT-PAT on a FlexConnect access point.
disable	Deletes NAT-PAT on a FlexConnect access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to enable central-DHCP, Override DNS, and NAT-PAT on a FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect central-dhcp 1 ap1250 enable override dns enable
 nat-pat enable
```

config ap flexconnect local-split

To configure a local-split tunnel on a FlexConnect access point, use the **config ap flexconnect local-split** command.

config ap flexconnect local-split *wlan_id cisco_ap* { **enable** | **disable** } **acl** *acl_name*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
cisco_ap	Name of the FlexConnect access point.
enable	Enables local-split tunnel on a FlexConnect access point.
disable	Disables local-split tunnel feature on a FlexConnect access point.
acl	Configures a FlexConnect local-split access control list.
acl_name	Name of the FlexConnect access control list.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command allows you to configure a local-split tunnel in a centrally switched WLAN using a FlexConnect ACL. A local split tunnel supports only for unicast Layer 4 IP traffic as NAT/PAT does not support multicast IP traffic.

Examples

The following example shows how to configure a local-split tunnel using a FlexConnect ACL:

```
(Cisco Controller) >config ap flexconnect local-split 6 AP2 enable acl flex6
```

config ap flexconnect policy

To configure a policy ACL on a FlexConnect access point, use the **config ap flexconnect policy** command.

config ap flexconnect policy {**add** | **delete**} *acl_name*

Syntax Description

add	Adds a policy ACL on a FlexConnect access point.
deletes	Deletes a policy ACL on a FlexConnect access point.
acl_name	Name of the ACL.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

Examples

The following example shows how to add a policy ACL on a FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect policy add acl1
```

config ap flexconnect radius auth set

To configure a primary or secondary RADIUS server for a specific FlexConnect access point, use the **config ap flexconnect radius auth set** command.

config ap flexconnect radius auth set {**primary** | **secondary**} *ip_address auth_port secret*

Syntax Description

primary	Specifies the primary RADIUS server for a specific FlexConnect access point.
secondary	Specifies the secondary RADIUS server for a specific FlexConnect access point.
ip_address	Name of the Cisco lightweight access point.
auth_port secret	Name of the port.
secret	RADIUS server secret.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to configure a primary RADIUS server for a specific access point:

```
(Cisco Controller) >config ap flexconnect radius auth set primary 192.12.12.1
```

config ap flexconnect vlan

To enable or disable VLAN tagging for a FlexConnect access, use the **config ap flexconnect vlan** command.

config ap flexconnect vlan {**enable** | **disable**} *cisco_ap*

Syntax Description

enable	Enables the access point’s VLAN tagging.
disable	Disables the access point’s VLAN tagging.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

Disabled. Once enabled, WLANs enabled for local switching inherit the VLAN assigned at the Cisco WLC.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

This example shows how to enable the access point’s VLAN tagging for a FlexConnect access:

```
(Cisco Controller) >config ap flexconnect vlan enable AP02
```

config ap flexconnect vlan add

To add a VLAN to a FlexConnect access point, use the **config ap flexconnect vlan add** command.

config ap flexconnect vlan add *vlan-id acl in-acl out-acl cisco_ap*

Syntax Description

vlan-id	VLAN identifier.
acl	ACL name that contains up to 32 alphanumeric characters.
in-acl	Inbound ACL name that contains up to 32 alphanumeric characters.
out-acl	Outbound ACL name that contains up to 32 alphanumeric characters.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to configure the FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect vlan add 21 acl inacl1 outacl1 ap1
```

config ap flexconnect vlan native

To configure a native VLAN for a FlexConnect access point, use the **config ap flexconnect vlan native** command.

config ap flexconnect vlan native *vlan-id cisco_ap*

Syntax Description

vlan-id	VLAN identifier.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to configure a native VLAN for a FlexConnect access point mode:

```
(Cisco Controller) >config ap flexconnect vlan native 6 AP02
```

config ap flexconnect vlan wlan

To assign a VLAN ID to a FlexConnect access point, use the **config ap flexconnect vlan wlan** command.

config ap flexconnect vlan wlan *ip_address vlan-id cisco_ap*

Syntax Description

ip_address	Name of the Cisco lightweight access point.
vlan-id	VLAN identifier.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

VLAN ID associated to the WLAN.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to assign a VLAN ID to a FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect vlan wlan 192.12.12.1 6 AP02
```

config ap flexconnect web-auth

To configure a FlexConnect ACL for external web authentication in locally switched WLANs, use the **config ap flexconnect web-auth** command.

config ap flexconnect web-auth wlan *wlan_id cisco_ap acl_name* { **enable** | **disable** }

Syntax Description

wlan	Specifies the wireless LAN to be configured with a FlexConnect ACL.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).
cisco_ap	Name of the FlexConnect access point.
acl_name	Name of the FlexConnect ACL.
enable	Enables the FlexConnect ACL on the locally switched wireless LAN.
disable	Disables the FlexConnect ACL on the locally switched wireless LAN.

Command Default

FlexConnect ACL for external web authentication in locally switched WLANs is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The FlexConnect ACLs that are specific to an AP have the highest priority. The FlexConnect ACLs that are specific to WLANs have the lowest priority.

Examples

The following example shows how to enable FlexConnect ACL for external web authentication on WLAN 6:

```
(Cisco Controller) >config ap flexconnect web-auth wlan 6 AP2 flexacl2 enable
```

config ap flexconnect web-policy acl

To configure a Web Policy FlexConnect ACL on an access point, use the **config ap flexconnect web-policy acl** command.

config ap flexconnect web-policy acl {**add** | **delete**} *acl_name*

Syntax Description

add	Adds a Web Policy FlexConnect ACL on an access point.
delete	Deletes Web Policy FlexConnect ACL on an access point.
acl_name	Name of the Web Policy FlexConnect ACL.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to add a Web Policy FlexConnect ACL on an access point:

```
(Cisco Controller) >config ap flexconnect web-policy acl add flexacl2
```

config ap flexconnect wlan

To configure a FlexConnect access point in a locally switched WLAN, use the **config ap flexconnect wlan** command.

config ap flexconnect wlan l2acl {**add** *wlan_id cisco_ap acl_name* | **delete** *wlan_id cisco_ap*}

Syntax Description

add	Adds a Layer 2 ACL to the FlexConnect access point.
wlan_id	Wireless LAN identifier from 1 to 512.
cisco_ap	Name of the Cisco lightweight access point.
acl_name	Layer 2 ACL name. The name can be up to 32 alphanumeric characters.
delete	Deletes a Layer 2 ACL from the FlexConnect access point.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

You can create a maximum of 16 rules for a Layer 2 ACL.

You can create a maximum of 64 Layer 2 ACLs on a controller.

A maximum of 16 Layer 2 ACLs are supported per AP because an AP supports a maximum of 16 WLANs.

Ensure that the Layer 2 ACL names do not conflict with the FlexConnect ACL names because an AP does not support the same Layer 2 and Layer 3 ACL names.

Examples

The following example shows how to configure a Layer 2 ACL on a FlexConnect access point.

```
(Cisco Controller) >config ap flexconnect wlan add 1 AP1600_1 acl_l2_1
```

config flexconnect acl

To apply access control lists that are configured on a FlexConnect access point, use the **config flexconnect acl** command.

config flexconnect acl {**apply** | **create** | **delete**} *acl_name*

Syntax Description

apply	Applies an ACL to the data path.
create	Creates an ACL.
delete	Deletes an ACL.
acl_name	ACL name that contains up to 32 alphanumeric characters.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to apply the ACL configured on a FlexConnect access point:

```
(Cisco Controller) >config flexconnect acl apply acl1
```

config flexconnect acl rule

To configure access control list (ACL) rules on a FlexConnect access point, use the **config flexconnect acl rule** command.

config flexconnect aclrule {**action** *rule_name rule_index* {**permit** | **deny**} | **add** *rule_name rule_index* | **change index** *rule_name old_index new_index* | **delete** *rule_name rule_index* | **destination address** *rule_name rule_index ip_address netmask* | **destination port range** *rule_name rule_index start_port end_port* | **direction** *rule_name rule_index* {**in** | **out** | **any**} | **dscp** *rule_name rule_index dscp* | **protocol** *rule_name rule_index protocol* | **source address** *rule_name rule_index ip_address netmask* | **source port range** *rule_name rule_index start_port end_port* | **swap index** *rule_name index_1 index_2*}

Syntax Description

action	Configures whether to permit or deny access.
rule_name	ACL name that contains up to 32 alphanumeric characters.
rule_index	Rule index between 1 and 32.
permit	Permits the rule action.
deny	Denies the rule action.
add	Adds a new rule.
change	Changes a rule’s index.
index	Specifies a rule index.
delete	Deletes a rule.
destination address	Configures a rule’s destination IP address and netmask.
ip_address	IP address of the rule.
netmask	Netmask of the rule.
start_port	Start port number (between 0 and 65535).
end_port	End port number (between 0 and 65535).
direction	Configures a rule’s direction to in, out, or any.
in	Configures a rule’s direction to in.
out	Configures a rule’s direction to out.
any	Configures a rule’s direction to any.
dscp	Configures a rule’s DSCP.

dscp	Number between 0 and 63, or **any**.
protocol	Configures a rule’s DSCP.
protocol	Number between 0 and 255, or **any**.
source address	Configures a rule’s source IP address and netmask.
source port range	Configures a rule’s source port range.
swap	Swaps two rules’ indices.
index_1	The rule first index to swap.
index_2	The rule index to swap the first index with.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

This example shows how to configure an ACL to permit access:

```
(Cisco Controller) >config flexconnect acl rule action lab1 4 permit
```

config flexconnect fallback-radio-shut

To configure the radio interface of an access point when the Ethernet link is not operational, use the **config flexconnect fallback-radio-shut** command.

config flexconnect fallback-radio-shut {{**disable**| **enable delay**} *delay-in-sec*

Syntax Description

disable	Disables the radio interface shutdown.
enable	Enables the radio interface shutdown.
delay	Specifies the delay for the interface after which the radio interface has to be shut down.
delay-in-sec	Delay duration, in seconds.

Command Default

The radio interface shutdown is disabled.

Command History

Release	Modification
7.6	This command was introduced.

Usage Guidelines

You can specify the delay duration only if you enable the radio interface shutdown.

Examples

The following example shows how to enable the radio interface shutdown after a delay duration of 5 seconds:

```
(Cisco Controller) >config flexconnect fallback-radio-shut enable delay 5
```

config flexconnect group

To add, delete, or configure a FlexConnect group, use the **config flexconnect group** command.

config flexconnect group *group_name* {**add** | **delete** | **ap** {**add** | **delete**} *ap-mac* | **radius** {**ap** {**authority** {**id** *hex_id* | **info** *auth_info*} | **disable** | **eap-fast** {**enable** | **disable**} | **enable** | **leap** {**enable** | **disable**} | **pac-timeout** *timeout* | **server-key** {**auto** | *key*} | **user** {**add** {*username password*} | **delete** *username*}}} | **server auth** {**add** | **delete**} {**primary** | **secondary**} *server_indexIP_address auth_port secret*} | **predownload** {**disable** | **enable**} | **master** *ap_name* | **slave** {**retry-count** *max_count* | **ap-name** *cisco_ap*} | **start** {**primary backup abort**} | **local-split** {**wlan** *wlan_id* **acl** *acl_name* {**enable** | **disable**}} | **multicast overridden-interface** {**enable** | **disable**} | **vlan** {**add** *vlan_id* **acl** *in-aclname out-aclname* | **delete** *vlan_id* } | **web-auth wlan** *wlan_id* **acl** *acl_name* {**enable** | **disable**} | **web-policy acl** {**add** | **delete**} *acl_name*}

config flexconnect group *group_name* **radius ap** {**eap-cert download** | **eap-tls** {**enable** | **disable**} | **peap** {**enable** | **disable**}}

config flexconnect group *group_name* **policy acl** {**add** | **delete**} *acl_name*

Syntax Description

group_name	Group name.
add	Adds a FlexConnect group.
delete	Deletes a FlexConnect group.
ap	Adds or deletes an access point to a FlexConnect group.
add	Adds an access point to a FlexConnect group.
delete	Deletes an access point to a FlexConnect group.
ap_mac	MAC address of the access point.
radius	Configures the RADIUS server for client authentication for a FlexConnect group.
ap	Configures an access point based RADIUS server for client authentication for a FlexConnect group.
authority	Configures the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) authority parameters.
id	Configures the authority identifier of the local EAP-FAST server.

hex_id	Authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal even number of characters.
info	Configures the authority identifier of the local EAP-FAST server in text format.
auth_info	Authority identifier of the local EAP-FAST server in text format.
disable	Disables an AP based RADIUS server.
eap-fast	Enables or disables Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) authentication.
enable	Enables EAP-FAST authentication.
disable	Disables EAP-FAST authentication.
enable	Enables AP based RADIUS Server.
leap	Enables or disables Lightweight Extensible Authentication Protocol (LEAP) authentication.
disable	Disables LEAP authentication.
enable	Enables LEAP authentication.
pac-timeout	Configures the EAP-FAST Protected Access Credential (PAC) timeout parameters.
timeout	PAC timeout in days. The range is from 2 to 4095. A value of 0 indicates that it is disabled.
server-key	Configures the EAP-FAST server key. The server key is used to encrypt and decrypt PACs.
auto	Automatically generates a random server key.
key	Key that disables efficient upgrade for a FlexConnect group.
user	Manages the user list at the AP-based RADIUS server.
add	Adds a user. You can configure a maximum of 100 users.
username	Username that is case-sensitive and alphanumeric and can be up to 24 characters.

password	Password of the user.
delete	Deletes a user.
server	Configures an external RADIUS server.
add	Adds an external RADIUS server.
delete	Deletes an external RADIUS server.
primary	Configures an external primary RADIUS server.
secondary	Configures an external secondary RADIUS server.
server_index	Index of the RADIUS server.
IP_address	IP address of the RADIUS server.
auth_port	Port address of the RADIUS server.
secret	Index of the RADIUS server.
predownload	Configures an efficient AP upgrade for the FlexConnect group. You can download an upgrade image to the access point from the controller without resetting the access point or losing network connectivity.
disable	Disables an efficient upgrade for a FlexConnect group.
enable	Enables an efficient upgrade for a FlexConnect group.
master	Manually designates an access point in the FlexConnect group as the master AP.
ap_name	Access point name.
slave	Manually designates an access point in the FlexConnect group as the slave AP.
retry-count	Configures the number of times the slave access point tries to predownload an image from the master.
max_count	Maximum number of times the slave access point tries to predownload an image from the master.

ap_name	Override the manually configured master.
cisco_ap	Name of the master access point.
start	Starts the predownload image upgrade for the FlexConnect group.
primary	Starts the predownload primary image upgrade for the FlexConnect group.
backup	Starts the predownload backup image upgrade for the FlexConnect group.
abort	Aborts the predownload image upgrade for the FlexConnect group.
local-split	Configures a local-split ACL on a FlexConnect AP group per WLAN.
wlan	Configures a WLAN for a local split ACL on a FlexConnect AP group.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).
acl	Configures a local split ACL on a FlexConnect AP group per WLAN.
acl_name	Name of the ACL.
multicast overridden-interface	Configures multicast across the Layer 2 broadcast domain on the overridden interface for locally switched clients.
vlan	Configures a VLAN to the FlexConnect group.
add	Adds a VLAN to the FlexConnect group.
vlan_id	VLAN identifier.
in-acl	Inbound ACL name that contains up to 32 alphanumeric characters.
out-acl	Outbound ACL name that contains up to 32 alphanumeric characters.
delete	Deletes a VLAN from the FlexConnect group.
web-auth	Configures a FlexConnect ACL for external web authentication.

wlan	Specifies the wireless LAN to be configured with a FlexConnect ACL.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).
cisco_ap	Name of the FlexConnect access point.
acl	Configures a FlexConnect ACLs.
web-policy	Configures a web policy FlexConnect ACL.
add	Adds a web policy FlexConnect ACL to the FlexConnect group.
delete	Deletes a web policy FlexConnect ACL from the FlexConnect group
eap-cert download	Downloads the EAP root and device certificate.
eap-tls	Enables or disables EAP-Transport Layer Security (EAP-TLS) authentication.
peap	Enables or disables Protected Extensible Authentication Protocol (PEAP) authentication.
policy acl	Configures policy ACL on the FlexConnect group.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can add up to 100 clients.

Beginning in Release 7.4 and later releases, the supported maximum number of RADIUS servers is 100.

Examples

The following example shows how to add a FlexConnect group for MAC address 192.12.1.2:

```
(Cisco Controller) >config flexconnect group 192.12.1.2 add
```

The following example shows how to add a RADIUS server as a primary server for a FlexConnect group with the server index number 1:

```
(Cisco Controller) >config flexconnect group 192.12.1.2 radius server add primary 1
```

The following example shows how to enable a local split ACL on a FlexConnect AP group for a WLAN:

```
(Cisco Controller) >config flexconnect group flexgroup1 local-split wlan 1 acl flexacl1
enable
```

config flexconnect group vlan

To configure VLAN for a FlexConnect group, use the **config flexconnect group vlan** command.

config flexconnect group *group_name* **vlan** {**add** *vlan-id* **acl** *in-aclname out-aclname* | **delete** *vlan-id*}

Syntax Description

group_name	FlexConnect group name.
add	Adds a VLAN for the FlexConnect group.
vlan-id	VLAN ID.
acl	Specifies an access control list.
in-aclname	In-bound ACL name.
out-aclname	Out-bound ACL name.
delete	Deletes a VLAN from the FlexConnect group.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to add VLAN ID 1 for the FlexConnect group myflexacl where the in-bound ACL name is in-acl and the out-bound ACL is out-acl:

```
(Cisco Controller) >config flexconnect group vlan myflexacl vlan add 1 acl in-acl out-acl
```

config flexconnect group web-auth

To configure Web-Auth ACL for a FlexConnect group, use the **config flexconnect group web-auth** command.

config flexconnect group *group_name* **web-auth wlan** *wlan-id* **acl** *acl-name* {**enable** | **disable**}

Syntax Description

group_name	FlexConnect group name.
wlan-id	WLAN ID.
acl-name	ACL name.
enable	Enables the Web-Auth ACL for a FlexConnect group.
disable	Disables the Web-Auth ACL for a FlexConnect group.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to enable Web-Auth ACL webauthacl for the FlexConnect group myflexacl on WLAN ID 1:

```
(Cisco Controller) >config flexconnect group myflexacl web-auth wlan 1 acl webauthacl enable
```

config flexconnect group web-policy

To configure Web Policy ACL for a FlexConnect group, use the **config flexconnect group web-policy** command.

config flexconnect group *group_name* **web-policy acl** {**add** | **delete**} *acl-name*

Syntax Description

group_name	FlexConnect group name.
add	Adds the Web Policy ACL.
delete	Deletes the Web Policy ACL.
acl-name	Name of the Web Policy ACL.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to add the Web Policy ACL mywebpolicyacl to the FlexConnect group myflexacl:

```
(Cisco Controller) >config flexconnect group myflexacl web-policy acl add mywebpolicyacl
```

config flexconnect join min-latency

To enable or disable the access point to choose the controller with the least latency when joining, use the **config flexconnect join min-latency** command.

config flexconnect join min-latency {**enable** | **disable**} *cisco_ap*

Syntax Description

enable	Enables the access point to choose the controller with the least latency when joining.
disable	Disables the access point to choose the controller with the least latency when joining.
cisco_ap	Cisco lightweight access point.

Command Default

The access point cannot choose the controller with the least latency when joining.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the controller that responds first. This command is supported only on the following controller releases:

- Cisco 2500 Series Controller
- Cisco 5500 Series Controller
- Cisco Flex 7500 Series Controllers
- Cisco 8500 Series Controllers
- Cisco Wireless Services Module 2

This configuration overrides the HA setting on the controller, and is applicable only for OEAP access points.

Examples

The following example shows how to enable the access point to choose the controller with the least latency when joining:

```
(Cisco Controller) >config flexconnect join min-latency enable CISCO_AP
```

config flexconnect office-extend

To configure FlexConnect mode for an OfficeExtend access point, use the **config flexconnect office-extend** command.

config flexconnect office-extend {{**enable** | **disable**} *cisco_ap* | **clear-personalssid-config** *cisco_ap*}

Syntax Description

enable	Enables the OfficeExtend mode for an access point.
disable	Disables the OfficeExtend mode for an access point.
clear-personalssid-config	Clears only the access point’s personal SSID.
cisco_ap	Cisco lightweight access point.

Command Default

OfficeExtend mode is enabled automatically when you enable FlexConnect mode on the access point.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Currently, only Cisco Aironet 1130 series and 1140 series access points that are joined to a Cisco 5500 Series Controller with a WPlus license can be configured to operate as OfficeExtend access points.

Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. OfficeExtend access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. You can enable or disable rogue detection for a specific access point or for all access points by using the **config rogue detection** command.

DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point or for all access points by using the **config ap link-encryption** command.

Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point by using the **config ap telnet** or **config ap ssh** command.

Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point or for all access points currently associated to the controller by using the **config ap link-latency** command.

Examples

The following example shows how to enable the office-extend mode for the access point Cisco_ap:

```
(Cisco Controller) >config flexconnect office-extend enable Cisco_ap
```

The following example shows how to clear only the access point's personal SSID for the access point Cisco_ap:

```
(Cisco Controller) >config flexconnect office-extend clear-personalssid-config Cisco_ap
```

config wlan flexconnect ap-auth

To configure local authentication of clients associated with FlexConnect on a locally switched WLAN, use the **config wlan flexconnect ap-auth** command.

config wlan flexconnect ap-auth *wlan_id* {**enable** | **disable**}

Syntax Description

ap-auth	Configures local authentication of clients associated with an FlexConnect on a locally switched WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables AP authentication on a WLAN.
disable	Disables AP authentication on a WLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Local switching must be enabled on the WLAN where you want to configure local authentication of clients associated with FlexConnect.

Examples

The following example shows how to enable authentication of clients associated with FlexConnect on a specified WLAN:

```
(Cisco Controller) >config wlan flexconnect ap-auth 6 enable
```

config wlan flexconnect learn-ipaddr

To enable or disable client IP address learning for the Cisco WLAN controller, use the **config wlan flexconnect learn-ipaddr** command.

config wlan flexconnect learn-ipaddr *wlan_id* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables client IP address learning on a wireless LAN.
disable	Disables client IP address learning on a wireless LAN.

Command Default

Disabled when the **config wlan flexconnect local-switching** command is disabled. Enabled when the **config wlan flexconnect local-switching** command is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If the client is configured with Layer 2 encryption, the controller cannot learn the client IP address, and the controller will periodically drop the client. Disable this option to keep the client connection without waiting to learn the client IP address.

Note The ability to disable IP address learning is not supported with FlexConnect central switching.

Examples

The following example shows how to disable client IP address learning for WLAN 6:

```
(Cisco Controller) >config wlan flexconnect learn-ipaddr disable 6
```

config wlan flexconnect local-switching

To configure local switching, central DHCP, NAT-PAT, or the override DNS option on a FlexConnect WLAN, use the **config wlan flexconnect local switching** command.

config wlan flexconnect local-switching *wlan_id* {**enable** | **disable**} { {**central-dhcp** {**enable** | **disable**} **nat-pat** {**enable** | **disable**} } | {**override option dns** { **enable** | **disable**} } }

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
enable	Enables local switching on a FlexConnect WLAN.
disable	Disables local switching on a FlexConnect WLAN.
central-dhcp	Configures central switching of DHCP packets on the local switching FlexConnect WLAN. When you enable this feature, the DHCP packets received from the AP are centrally switched to the controller and forwarded to the corresponding VLAN based on the AP and the SSID.
enable	Enables central DHCP on a FlexConnect WLAN.
disable	Disables central DHCP on a FlexConnect WLAN.
nat-pat	Configures Network Address Translation (NAT) and Port Address Translation (PAT) on the local switching FlexConnect WLAN.
enable	Enables NAT-PAT on the FlexConnect WLAN.
disable	Disables NAT-PAT on the FlexConnect WLAN.
override	Specifies the DHCP override options on the FlexConnect WLAN.
option dns	Specifies the override DNS option on the FlexConnect WLAN. When you override this option, the clients get their DNS server IP address from the AP, not from the controller.
enable	Enables the override DNS option on the FlexConnect WLAN.
disable	Disables the override DNS option on the FlexConnect WLAN.

Command Default

This feature is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enable the **config wlan flexconnect local-switching** command, the **config wlan flexconnect learn-ipaddr** command is enabled by default.

Note The ability to disable IP address learning is not supported with FlexConnect central switching.

Examples

The following example shows how to enable WLAN 6 for local switching and enable central DHCP and NAT-PAT:

```
(Cisco Controller) >config wlan flexconnect local-switching 6 enable central-dhcp enable
nat-pat enable
```

The following example shows how to enable the override DNS option on WLAN 6:

```
(Cisco Controller) >config wlan flexconnect local-switching 6 override option dns enable
```

config wlan flexconnect vlan-central-switching

To configure central switching on a locally switched WLAN, use the **config wlan flexconnect vlan-central-switching** command.

config wlan flexconnect vlan-central-switching *wlan_id* { **enable** | **disable** }

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables central switching on a locally switched wireless LAN.
disable	Disables central switching on a locally switched wireless LAN.

Command Default

Central switching is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You must enable Flexconnect local switching to enable VLAN central switching. When you enable WLAN central switching, the access point bridges the traffic locally if the WLAN is configured on the local IEEE 802.1Q link. If the VLAN is not configured on the access point, the AP tunnels the traffic back to the controller and the controller bridges the traffic to the corresponding VLAN.

WLAN central switching does not support:

- FlexConnect local authentication.
- Layer 3 roaming of local switching client.

Examples

The following example shows how to enable WLAN 6 for central switching:

```
(Cisco Controller) >config wlan flexconnect vlan-central-switching 6 enable
```

Integrated Management Module Commands in Cisco Flex 7500 Series Controllers

Use the **imm** commands to manage the Integrated Management Module (IMM) in the Cisco Flex 7500 Series Controllers.

imm address

To configure the static IP address of the IMM, use the **imm address** command.

imm address *ip-addr netmask gateway*

Syntax Description

ip-addr	IP address of the IMM
netmask	Netmask of the IMM
gateway	Gateway of the IMM

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to set the static IP address of an IMM:

```
(Cisco Controller) >imm address 209.165.200.225 255.255.255.224 10.1.1.1
```

imm dhcp

To configure DHCP for the IMM, use the **imm dhcp** command.

imm dhcp {**enable** | **disable** | **fallback**}

Syntax Description

enable	Enables DHCP for the IMM
disable	Disables DHCP for the IMM
fallback	Enables DHCP for the IMM, but if it fails, then uses static IP of the IMM

Command Default

DHCP for IMM is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to enable DHCP for the IMM:

```
(Cisco Controller) >imm dhcp enable
```

imm mode

To configure the IMM mode, use the **imm mode** command.

imm mode {**shared** | **dedicated**}

Syntax Description

shared	Sets IMM in shared mode
dedicated	Sets IMM in dedicated mode

Command Default

Dedicated

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to set the IMM in shared mode:

```
(Cisco Controller) >imm mode
```

imm restart

To restart the IMM, use the **imm restart** command.

imm restart

Syntax Description

restart	Saves your settings and restarts the IMM

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

imm summary

To view the IMM parameters, use the **imm summary** command.

imm summary

Syntax Description

summary	Lists the IMM parameters

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows a typical summary of the IMM:

```
(Cisco Controller) >imm summary
User ID..........................................username1
Mode............................................. Shared
DHCP............................................. Enabled
IP Address....................................... 209.165.200.225
Subnet Mask...................................... 255.255.255.224
Gateway.......................................... 10.1.1.1
```

imm username

To configure the logon credentials for an IMM user, use the **imm username** command.

imm username *username password*

Syntax Description

username	Username for the user
password	Password for the user

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to set the logon credentials of an IMM user:

```
(Cisco Controller) >imm username username1 password1
```

debug Commands

debug capwap reap

To configure the debugging of Control and Provisioning of Wireless Access Points (CAPWAP) settings on a FlexConnect access point, use the **debug capwap reap** command.

debug capwap reap [**mgmt** | **load**]

Syntax Description

mgmt	(Optional) Configures the debugging for client authentication and association messages.
load	(Optional) Configures the debugging for payload activities, which is useful when the FlexConnect access point boots up in standalone mode.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to configure the debugging of FlexConnect client authentication and association messages:

```
(Cisco Controller) >debug capwap reap mgmt
```

debug dot11 mgmt interface

To configure debugging of 802.11 management interface events, use the **debug dot11 mgmt interface** command.

debug dot11 mgmt interface

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to debug 802.11 management interface events:

```
(Cisco Controller) >debug dot11 mgmt interface
```

debug dot11 mgmt msg

To configure debugging of 802.11 management messages, use the **debug dot11 mgmt msg** command.

debug dot11 mgmt msg

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

This example shows how to debug dot11 management messages:

```
(Cisco Controller) >debug dot11 mgmt msg
```

debug dot11 mgmt ssid

To configure debugging of 802.11 SSID management events, use the **debug dot11 mgmt ssid** command.

debug dot11 mgmt ssid

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to configure the debugging of 802.11 SSID management events:

```
(Cisco Controller) >debug dot11 mgmt ssid
```

debug dot11 mgmt state-machine

To configure debugging of the 802.11 state machine, use the **debug dot11 mgmt state-machine** command.

debug dot11 mgmt state-machine

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to configure the debugging of 802.11 state machine:

```
(Cisco Controller) >debug dot11 mgmt state-machine
```

debug dot11 mgmt station

To configure the debugging of the management station settings, use the **debug dot11 mgmt station** command.

debug dot11 mgmt station

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to configure the debugging of the management station settings:

```
(Cisco Controller) >debug dot11 mgmt station
```

debug flexconnect aaa

To configure debugging of FlexConnect backup RADIUS server events or errors, use the **debug flexconnect aaa** command.

debug flexconnect aaa {**event** | **error**} {**enable** | **disable**}

Syntax Description

event	Configures the debugging for FlexConnect RADIUS server events.
error	Configures the debugging for FlexConnect RADIUS server errors.
enable	Enables the debugging of FlexConnect RADIUS server settings.
disable	Disables the debugging of FlexConnect RADIUS server settings.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to enable the debugging of FlexConnect RADIUS server events:

```
(Cisco Controller) >debug flexconnect aaa event enable
```

debug flexconnect acl

Configures debugging of FlexConnect access control lists (ACLs), use the **debug flexconnect acl** command.

debug flexconnect acl {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of FlexConnect ACLs.
disable	Disables the debugging of FlexConnect ACLs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to enable the debugging of FlexConnect ACLs:

```
(Cisco Controller) >debug flexconnect acl enable
```

debug flexconnect cckm

Configure debugging of FlexConnect Cisco Centralized Key Management (CCKM) fast roaming, use the **debug flexconnect cckm** command.

debug flexconnect cckm {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of FlexConnect CCKM fast roaming settings.
disable	Disables the debugging of FlexConnect CCKM fast roaming settings.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to enable the debugging of FlexConnect CCKM fast roaming events:

```
(Cisco Controller) >debug flexconnect cckm event enable
```

debug flexconnect group

To configure debugging of FlexConnect access point groups, use the **debug flexconnect group** command.

debug flexconnect group {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of FlexConnect access point groups.
disable	Disables the debugging of FlexConnect access point groups.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to enable the debugging of FlexConnect access point groups:

```
(Cisco Controller) >debug flexconnect group enable
```

debug pem

To configure debugging of the access policy manager, use the **debug pem** command.

debug pem {**events** | **state**} {**enable** | **disable**}

Syntax Description

events	Configures the debugging of the policy manager events.
state	Configures the debugging of the policy manager state machine.
enable	Enables the debugging of the access policy manager.
disable	Disables the debugging of the access policy manager.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to enable the debugging of the access policy manager:

```
(Cisco Controller) >debug pem state enable
```